

Motion till Östra-Nylands Vårdsområde, Borgå.

Hur jobba med DIGI-KLINIK varifrån som helst.

För att kunna säkra patientuppgifter och GDPR enligt lagen bör man vara ytterst säker med den digitala processen både på arbetsplatsen och ifall den skulle finnas i hemmet.

Här är det i sin enklaste form: Att arbeta så säkert som möjligt.

1. Arbetsgivarens lap-top. Endast för envars personligt bruk 100%.
2. På lap-toppen endast de nödvändigaste programmen insatta samt restriktioner att sätta in sk egn program.
3. Bästa möjliga brandmur samt routrar. Typ Mikrotik. Uppdateras med tiden.
4. Bästa möjliga anti-virus program som uppdateras hela tiden. Typ F-Secure.
5. Kontinuerlig skolning om de risker som förekommer och nya hot som uppstår.
6. Skolning om riskerna med diverse kort och hemligheter samt hur hålla allt under kontroll.

What is needed to secure workstation at home using Citrix remote line to database in the cloud?

Securing a workstation at home that connects to a Citrix remote line to a database in the cloud requires additional security measures to protect the confidentiality, integrity, and availability of the data being accessed. Here are some essential steps you can take:

1. Use a secure Citrix connection: Ensure that your Citrix connection is configured to use SSL/TLS encryption to secure the communication between your workstation and the Citrix server.
2. Implement multi-factor authentication: Use multi-factor authentication to add an extra layer of security to your Citrix login process. This can be done through various methods, such as smart cards, biometrics, or tokens.
3. Use a VPN for added security: Consider using a VPN to encrypt your internet connection and ensure that your data is transmitted securely between your workstation and the Citrix server.
4. Use antivirus and anti-malware software: Install and regularly update antivirus and anti-malware software on your workstation to detect and prevent malware and viruses from infecting your computer.
5. Configure firewall settings: Configure your firewall settings to allow access only to the necessary ports and protocols needed for your Citrix connection.
6. Keep your workstation and software up to date: Regularly update your operating system, web browsers, and other software applications to ensure that they are protected against known vulnerabilities and exploits.
7. Limit access to your workstation: Ensure that your workstation is physically secured and that access to it is limited to authorized users only.

8. Use secure passwords: Create strong, unique passwords for all your accounts, including your Citrix login, and use a password manager to securely store them.

By following these steps, you can significantly reduce the risk of cyber threats and protect your workstation, data, and the remote database accessed through Citrix. It's also important to regularly review and update your security measures to stay protected against evolving threats.

Föreslår att Vårdsområdet uppgör strikta regler för hur den Digitala patient processen sköts och att dessa regler kommer till vårdsområdets styrelse för godkännande.

Alternativ är att hela den digitala vården sättes på yttre anbudstävlan och kommer i framtiden att skötas av utomstående bolag.

Borgå

30.3.2023

Bernhard Edgren

Läkare, Styrelsemedlem, Fullmäktige.



Bernhard Edgren Doctor/GP  
Special Comp. in Travel Medicine  
Reg. nr. 200638 ☎ +358 (0) 430490  
be@triuno.com • www.triuno.com